AMENDMENTS TO CLAIMS

Please amend the claims as indicated hereinafter.

1. (Previously Presented) A method, comprising the computer-implemented steps of:
in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
determining a user identifier associated with the network device that has caused a security event in the network;
in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;
wherein the second subset of addresses is different from the first subset of addresses; and
configuring one or more security restrictions with respect to the second network address.

2. (Original) A method as recited in Claim 1, further comprising the steps of:
receiving information identifying the security event in the network;
correlating the security event information with network user information to result in determining the user identifier associated with the network device.

3. (Previously Presented) A method as recited in Claim 44, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the step of causing the network device to acquire the second network address comprises resetting

a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.

4. (Previously Presented) A method as recited in Claim 44, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the step of causing the network device to acquire the second network address comprises issuing a DHCP FORCE_RENEW message to the network device.

5. (Previously Presented) A method as recited in Claim 44, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the step of causing the network device to acquire the second network address comprises prompting the network device to request a new network address using DHCP.

6. (Previously Presented) A method as recited in Claim 1, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the step of causing the network device to acquire the second network address comprises waiting for expiration of a lease for a current network address of the network device.

7. (Previously Presented) A method as recited in Claim 1, wherein the step of causing the network device to acquire the second network address comprises the step of providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.

8. (Original) A method as recited in Claim 7, further comprising the step of publishing information describing characteristics of the special IP subnet to network service providers.

9. (Previously Presented) A method as recited in Claim 1, wherein the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address.

10. (Previously Presented) A method as recited in Claim 1, wherein the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL

associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the second network address.

11. (Original) A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller.

12. (Previously presented) A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, and if not, removing the user from the second specified pool.

13. (Original) A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated with a trusted customer of a network service provider.

14–17. (Canceled)

18. (Previously Presented) A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

determining a user identifier associated with the network device that has caused a security event in the network;

in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing,

extraneous requests for network addresses, and possible MAC address spoofing;

wherein the second subset of addresses is different from the first subset of addresses; and

configuring one or more security restrictions with respect to the second network address.

19. (Previously Presented) An apparatus, comprising:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

means for determining a user identifier associated with the network device that has caused a security event in the network;

means for, in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;

wherein the second subset of addresses is different from the first subset of addresses; and

means for configuring one or more security restrictions with respect to the second network address.

20. (Previously Presented) An apparatus, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

in a security controller that is coupled, through the data network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

determining a user identifier associated with the network device that has caused a security event in the network;

in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;

wherein the second subset of addresses is different from the first subset of addresses; and

configuring one or more security restrictions with respect to the second network address.

21–29. (Canceled)

30. (Previously Presented) The apparatus of claim 20, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the instructions which when executed cause the network device to acquire a second network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.

31. (Previously Presented) The apparatus of claim 20, wherein instructions which when executed cause the network device to acquire a second network address comprise instructions which when executed cause providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.

32. (Previously Presented) The apparatus of claim 20, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the instructions which when executed cause the network device to acquire a second network address comprise instructions which when executed cause issuing a DHCP FORCE_RENEW message to the network device.

33. (Previously Presented) The computer-readable storage medium of claim 18, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the instructions which, when executed, cause the network device to acquire the second network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.

34. (Previously Presented) The computer-readable storage medium of claim 18, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the instructions which when executed cause the network device to acquire the second network address comprise instructions which when executed cause issuing a DHCP FORCE_RENEW message to the network device.

35. (Previously Presented) The computer-readable storage medium of claim 18, wherein instructions which when executed cause the network device to acquire a second network address comprise instructions which when executed cause providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.

36. (Previously Presented) The apparatus of claim 19, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and

wherein the means for causing the network device to acquire the second network address comprise means for resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.

37. (Previously Presented) The apparatus of claim 19, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the means for causing the network device to acquire the second network address comprise means for issuing a DHCP FORCE_RENEW message to the network device.

38. (Previously Presented) The apparatus of claim 19, wherein the means for causing the network device to acquire a new network address comprise means for providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.

39.–42. (Canceled)

43. (Previously Presented) The method of Claim 1, wherein causing the network device to acquire a second network address comprises performing an action that causes the network device to request a new network address.

44. (Previously Presented) A method, comprising the computer-implemented steps of:
in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
in response to a security event in the network, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;

wherein causing the network device to acquire a second network address comprises performing an action that causes the network device to request a new network address;

wherein the second subset of addresses is different from the first subset of addresses; and

configuring one or more security restrictions with respect to the new network address.

45. (New) The apparatus as recited in Claim 20, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

receiving information identifying the security event in the network;

correlating the security event information with network user information to result in determining the user identifier associated with the network device.

46. (New) The apparatus as recited in Claim 20, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein causing the network device to acquire the second network address comprises prompting the network device to request a new network address using DHCP.

47. (New) The apparatus as recited in Claim 20, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein causing the network device to acquire the second network address comprises waiting for expiration of a lease for a current network address of the network device.

48. (New) The apparatus as recited in Claim 31, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

publishing information describing characteristics of the special IP subnet to network service providers.

49. (New) The apparatus as recited in Claim 20, wherein configuring security restrictions comprises modifying an internet protocol (IP) access control list (ACL) associated with a port

that is coupled to the network device to permit entry of IP traffic from only the second network address.

50. (New) The apparatus as recited in Claim 20, wherein configuring security restrictions comprises modifying a media access control (MAC) ACL associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the second network address.

51. (New) The apparatus as recited in Claim 20, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller.

52. (New) The apparatus as recited in Claim 20, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

determining whether a malicious act caused the security event, and if not, removing the user from the second specified pool.

53. (New) The apparatus as recited in Claim 20, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated with a trusted customer of a network service provider.

54. (New) The apparatus as recited in Claim 20, wherein causing the network device to acquire a second network address comprises performing an action that causes the network device to request a new network address.

55. (New) The apparatus as recited in Claim 19, further comprising:

means for receiving information identifying the security event in the network; and

means for correlating the security event information with network user information to result in determining the user identifier associated with the network device.

56. (New) The apparatus as recited in Claim 19, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the means for causing the network device to acquire the second network address comprises means for prompting the network device to request a new network address using DHCP.

57. (New) The apparatus as recited in Claim 19, wherein the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the means for causing the network device to acquire the second network address comprises waiting for expiration of a lease for a current network address of the network device.

58. (New) The apparatus as recited in Claim 38, further comprising:
means for publishing information describing characteristics of the special IP subnet to network service providers.

59. (New) The apparatus as recited in Claim 19, wherein the means for configuring security restrictions comprises means for modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address.

60. (New) The apparatus as recited in Claim 19, wherein the means for configuring security restrictions comprises means for modifying a media access control (MAC) ACL associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the second network address.

61. (New) The apparatus as recited in Claim 19, further comprising:
means for determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller.

62. (New) The apparatus as recited in Claim 19, further comprising:
means for determining whether a malicious act caused the security event, and if not, removing the user from the second specified pool.

63. (New) The apparatus as recited in Claim 19, further comprising:

means for determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated with a trusted customer of a network service provider.

64. (New) The apparatus as recited in Claim 19, wherein the means for causing the network device to acquire a second network address comprises means for performing an action that causes the network device to request a new network address.